

Response under 37 C.F.R. § 1.116
Serial No. 10/029,378
Page 2

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. (Currently Amended) A method for use by ~~nodes~~ a node to route packet traffic through a multiple-hop wireless communications network, the method comprising:
detecting interference in the form of signals that are attempting to interfere with packet-switched communications at the node that are carried by radio frequency (RF) over the multiple-hop wireless communications network; and
determining, in response to information related to the detected interference, a route for transmitting packets through the multiple-hop wireless communications network that mitigates the effect of the interference on the packets.
2. (Previously Presented) The method of claim 1 further comprising the step of identifying a source of the interference to be a node in the multiple-hop wireless communications network, and wherein the determined route excludes the node.
3. (Previously Presented) The method of claim 1 further comprising the step of identifying one or more nodes interfered with by the interference, and wherein the determined route excludes one or more of the interfered-with nodes.
4. (Previously Presented) The method of claim 1 further comprising the step of approximating a geographical location of a source of the interference, and wherein the determined route excludes one or more nodes near that location.
5. (Original) The method of claim 1 wherein the step of detecting interference includes determining that signals received by a node are of an unauthorized protocol.
6. (Original) The method of claim 1 wherein the step of detecting interference includes determining that an address included in signals received by a node is an address of a known unauthorized source.
7. (Original) The method of claim 1 wherein the step of detecting interference

Response under 37 C.F.R. § 1.116
Serial No. 10/029,378
Page 3

includes determining that a protocol header included in signals received by a node has invalid information.

8. (Original) The method of claim 1 further comprising operating a protocol at a physical layer of a protocol stack that detects the interference.

9. (Previously Presented) The method of claim 8 wherein the step of determining a route is performed by a network layer protocol in the protocol stack in response to a notification from the physical layer protocol of the interference.

10. (Original) The method of claim 1 further comprising operating a protocol at a data link layer of a protocol stack that detects the interference.

11. (Previously Presented) The method of claim 10 wherein the step of determining a route is performed by a network layer protocol in the protocol stack in response to a notification from the data layer protocol of the interference.

12. (Original) The method of claim 1 further comprising operating a protocol at a network layer of a protocol stack that detects suspicious communication behavior.

13. (Original) The method of claim 12 wherein the step of detecting interference is accomplished by a physical layer protocol of the protocol stack in response to a notification from the network layer protocol of the suspicious network behavior.

14. (Previously Presented) The method of claim 1 further comprising adjusting an antenna pattern of a node in the wireless communications network in response to detecting the interference.

15. (Previously Presented) The method of claim 14 wherein the step of adjusting the antenna pattern includes forming a null in the antenna pattern in a direction of the interference.

16. (Original) The method of claim 1 further comprising disseminating to nodes in the multiple hop wireless communications network information related to the detecting of the interference.

Response under 37 C.F.R. § 1.116
Serial No. 10/029,378
Page 4

17. (Original) The method of claim 16 wherein the disseminated information is an identity associated with a source of the interference.

18. (Original) The method of claim 16 wherein the disseminated information is an identity associated with a node in the multiple hop wireless communications network that is being interfered with by the interference.

19. (Original) The method of claim 1 identifying a source of the interference to be a node in the multiple-hop wireless communications network, calculating a cost function for a plurality of routes from a sending node to a destination node that exclude the interfering node, and selecting the route with a lowest cost function.

20. (Original) The method of claim 1 wherein the nodes in the wireless communications network operate according to one of the protocols selected from the group consisting of IEEE 802.11, BLUETOOTH, HYPERLAN and HOMERF.

21. (Original) A protocol stack for use by a node to communicate over a wireless communications network, the protocol stack comprising:

a radio frequency (RF) physical layer for detecting signals that are attempting to interfere with packet-switched communications at the node, the RF physical layer producing a signal that indicates that interference has been detected; and

a network layer receiving the signal from the RF physical layer and producing an alternate route of packets through the wireless communications network in response to the signal.

22. (Original) The protocol stack of claim 21 further comprising a data link layer for checking for errors packets received by the node and sending a signal to the network layer when interference has been detected.